Release Notes for Cisco 802 IDSL and 804 IDSL Routers for Cisco IOS Release 12.0(5)T

December 6, 1999

Cisco IOS Release 12.0(5)T

Text Part Number 78-10388-01

These release notes for the Cisco 802 IDSL and Cisco 804 IDSL routers support Cisco IOS Release 12.0 T, up to and including Release 12.0(5)T. These release notes are updated as needed to describe new features, memory requirements, hardware support, software platform deferrals, and changes to the microcode or modem code and related documents.

Note The term ISDN represents an Integrated Services Digital Network (ISDN). The term IDSL represents an ISDN digital subscriber line (IDSL).

For a list of the software caveats that apply to Release 12.0 T, see the *Caveats for Cisco IOS Release 12.0 T* document that accompanies these release notes. The caveats document is updated for every maintenance release and is located on Cisco Connection Online (CCO) and the Documentation CD-ROM. Use these release notes with *Cross-Platform Release Notes for Cisco IOS Release 12.0* on CCO and the Documentation CD-ROM.

Note Cisco 802 IDSL and Cisco 804 IDSL routers require Cisco IOS release 12.0(5)T software or above. In addition, the software images described in these release notes support the Cisco 802 IDSL and Cisco 804 IDSL routers only; they do not support the Cisco 801–804 routers or the Cisco 805 router.

CISCO SYSTEMS

Corporate Headquarters: Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Copyright © 1999. Cisco Systems, Inc. All rights reserved.

Contents

These release notes describe the following topics:

- System Requirements, page 2
- New and Changed Information, page 7
- Important Notes, page 11
- Caveats, page 17
- Related Documentation, page 17
- Service and Support, page 23
- Cisco Connection Online, page 24
- Documentation CD-ROM, page 24

System Requirements

This section describes the system requirements for Release 12.0(5)T:

- Memory Requirements, page 2
- Hardware Supported, page 2
- Determining the Software Version, page 3
- Upgrading to a New Software Release, page 3
- Feature Set Tables, page 4

Memory Requirements

Table 1 Memory Requirements for the Cisco 802 IDSL and 804 IDSL Routers

Platforms	Feature Sets[1]	Image Name	Software Image	Required Flash Memory	Required DRAM Memory	Runs from
Cisco 802 IDSL and Cisco 804 IDSL	IP Feature Sets	Internet DSL	c800-y6-mw	8 MB	4 MB	RAM
		Internet DSL/FW/IPSec56	c800-osy656i-mw	8 MB	8 MB	RAM
		Internet DSL/IPX/FW/ IPSec56	c800-nosy656i-mw	8 MB	8 MB	RAM

1. If you need to upgrade the main memory for your Cisco series router, be sure to order the upgrade specific to your router.

Hardware Supported

Cisco IOS Release 12.0(5)T supports the following Cisco 800 series routers:

- Cisco 802 IDSL
- Cisco 804 IDSL

Table 2 summarizes the Cisco 802 IDSL and 804 IDSL routers and the ports that each model offers.

Table 2 Cisco 802 IDSL and 804 IDSL Series Router Ports

Router	Ethernet Ports	ISDN Ports	Console Ports
Cisco 802	One 10BaseT (RJ-45)	ISDN BRI U, integrated Network Termination 1 (NT-1) (RJ-45)	RJ-45
Cisco 804	Four-port 10BaseT (RJ-45) hub	ISDN BRI U, integrated NT-1 (RJ-45)	RJ-45

The Cisco 802 IDSL and 804 IDSL routers provide the following key hardware features:

- Flash memory: the default is 8 MB, expandable to 12 MB.
- Dynamic RAM: the default is 4 MB, expandable to 12 MB.
- Color-coded ports and cable reduce the chance of cabling errors.
- Routers can be stacked or mounted on a wall.

Determining the Software Version

To determine the version of Cisco IOS software running on your Cisco 800 series, log in to the router and enter the **show version** EXEC command:

```
router> show version
Cisco Internetwork Operating System Software
IOS (tm) 800 Software (C800-Y6-MW), Version 12.0(5)T, RELEASE SOFTWARE
```

Upgrading to a New Software Release

For information on upgrading to a new software release, see the product bulletin *Cisco IOS Software Release 12.0 T Upgrade Paths and Packaging Simplification (#819: 1/99)* on CCO at:

Service & Support: **Software Center**: **Product Information**: **Product Bulletins**: **Software**: **Cisco IOS 12.0**: **Cisco IOS Software Release 12.0T Upgrade - No. 819**

Feature Set Tables

The Cisco IOS software is packaged in feature sets consisting of software images—depending on the platform. Each feature set contains a specific set of Cisco IOS features. Release 12.0 T supports the same feature sets as Release 12.0, but Release 12.0 T can include new features supported by the Cisco 802 IDSL and 804 IDSL routers.

Table 3 Feature Sets Supported by the Cisco 802 IDSL and 804 IDSL Routers

Feature Sets	Image Names	Feature Set Matrix Term	Software Image	Platforms	In[1]
IP Feature Sets	Internet DSL	Basic[2]	c800-y6-mw	Cisco 802 IDSL Cisco 804 IDSL	(5)
	Internet DSL/FW/IPSec56	Basic, IPSec 56[3]	c800-osy656i-mw	Cisco 802 IDSL Cisco 804 IDSL	(5)
	Internet DSL/IPX/FW/ IPSec56	Basic, IPSec 56	c800-nosy656i-mw	Cisco 802 IDSL Cisco 804 IDSL	(5)

1. The number in the “In” column indicates the Cisco IOS release when the image was first introduced. For example, (5) means an image was introduced in Release 12.0(5)T. If a cell in this column is empty, the interface was included in the initial base release.
2. This feature set is offered in the basic feature set.
3. This feature set is offered in the encryption feature sets, which consist of IPSec 56-bit (Plus IPSec 56) data encryption feature sets.

Caution Cisco IOS images with strong encryption (including, but not limited to 168-bit (3DES) data encryption feature sets) are subject to United States government export controls and have limited distribution. Strong encryption images to be installed outside the United States may require an export license. Customer orders may be denied or subject to delay due to United States government regulations. When applicable, the purchaser or the user must obtain local import and use authorizations for all encryption strengths. Contact your sales representative or distributor for more information, or send an e-mail to export@cisco.com.

Table 4 and Table 5 list the features and feature sets supported by the Cisco 800 routers in Cisco IOS Release 12.0(5)T and use the following conventions:

- Yes—The feature is supported in the software image.
- No—The feature is not supported in the software image.
- In—The number in the “In” column indicates the Cisco IOS release in which the feature was introduced. For example, (5) means a feature was introduced in Release 12.0(5)T. If a cell in this column is empty, the feature was included in the initial base release.

Note The feature set tables only contain a selected list of features. These tables are not cumulative—nor do they list all the features in each image.

Table 4 Feature List by Feature Set for the Cisco 802 IDSL and 804 IDSL Routers

Features	In	Feature Set		
		Internet DSL	Internet DSL/FW/ IPSec56	Internet DSL/IPX/FW / IPSec56
Analog Telephone Features				
Basic & Supplementary Features		No	No	No
Basic Security				
Extended Access Control Lists		Yes	Yes	Yes
Full NAT (including one-to-one, many-to-many, & many-to-one)		Yes	Yes	Yes
GRE Tunneling		No	No	No
Local Password		Yes	Yes	Yes
MS-CHAP		No	No	No
PAP, CHAP		Yes	Yes	Yes
Route and Router Authentication		No	No	No
Static Translation		Yes	Yes	Yes
Token Card Authentication		Yes	Yes	Yes
Ease of Use & Deployment				
Auto SPID/SWITCH Connection	(3)	No	No	No
Cisco Fast Step Equivalent		No	No	No
Configuration Express		Yes	Yes	Yes
DHCP Server	(3)	Yes	Yes	Yes
IPCP including Address Negotiations		Yes	Yes	Yes
TFTP Client /Server		Yes	Yes	Yes
Enhanced Security				
IOS Firewall Including:				
Context Based Access Control Lists/Stateful Inspection	(5)	No	Yes	Yes
Denial of Service Detection	(5)	No	Yes	Yes
Java Blocking	(5)	No	Yes	Yes
Real time alerts	(5)	No	Yes	Yes
IPSec Encryption w/ 56bit DES	(5)	No	Yes	Yes
L2TP	(5)	No	Yes	Yes
LAN				
Filtering		Yes	Yes	Yes
IP		Yes	Yes	Yes

Table 4 Feature List by Feature Set for the Cisco 802 IDSL and 804 IDSL Routers (continued)

Features	In	Feature Set		
		Internet DSL	Internet DSL/FW/ IPSec56	Internet DSL/IPX/FW / IPSec56
IPX WAN		No	No	Yes
NetBIOS Access Lists, Name Caching		Yes	Yes	Yes
Transparent Bridging (including Spanning Tree)		Yes	Yes	Yes
Management				
BootP Server		No	No	No
DHCP/BootP Relay	(3)	Yes	Yes	Yes
Interactive (IOS) Debug		Yes	Yes	Yes
Interface Statistics		Yes	Yes	Yes
Loopback Testing		Yes	Yes	Yes
Monitor Tool		Yes	Yes	Yes
Performance History		Yes	Yes	Yes
SNTP		No	No	No
SNMP Read & Write (set & read MIB's)		No	No	No
SNMP Read only		Yes	Yes	Yes
Syslog		No	No	No
TACAS+		No	No	No
Telnet, Console Port		Yes	Yes	Yes
User programmable Menu System		No	No	No
Routing				
IP Enhanced IGRP		No	No	No
IP Multicast (relay only)		No	No	No
IP-Policy Routing		No	No	No
IPX WAN		No	No	Yes
RIP		Yes	Yes	Yes
RIPv2,		Yes	Yes	Yes
Triggered RIP		Yes	Yes	Yes
WAN				
Frame Relay (Leased Line Only)		Yes	Yes	Yes
HDLC		Yes	Yes	Yes
IDSL		Yes	Yes	Yes
ISDN		No	No	No
ISDN Lease Line		Yes	Yes	Yes
ML-PPP		Yes	Yes	Yes
PPP		Yes	Yes	Yes

Table 4 Feature List by Feature Set for the Cisco 802 IDSL and 804 IDSL Routers (continued)

Features	In	Feature Set		
		Internet DSL	Internet DSL/FW/ IPSec56	Internet DSL/IPX/FW / IPSec56
Selectable settings up to 144Kbps		Yes	Yes	Yes
Virtual Templates		No	No	No
WAN Optimization				
AO/DI		No	No	No
Bandwidth on Demand		No	No	No
Dial on Demand Routing		No	No	No
Fair Queuing		Yes	Yes	Yes
IPX & SPX Spoofing		No	No	Yes
ISDN Caller ID Call-back		No	No	No
Snapshot Routing		No	No	No
Stac Compression		Yes	Yes	Yes
Weighted Fair Queuing		No	No	No
X.25 over D Channel		No	No	No

New and Changed Information

The following sections list the new hardware and software features supported by the Cisco 802 IDSL and 804 IDSL routers for Release 12.0 T.

New Hardware Features in Release 12.0(5)T

The following new hardware is supported by the Cisco 802 IDSL and 804 IDSL routers in Release 12.0(5)T and later releases.

Support for Cisco 802 IDSL and 804 IDSL Routers

Release 12.0(5)T includes support for the Cisco 802 IDSL and 804 IDSL routers.

New Software Features in Release 12.0(5)T

The following new software enhancements are supported by the Cisco 802 IDSL and 804 IDSL routers in Release 12.0(5)T and later releases.

Cisco IOS Firewall Feature Set for the Cisco 802 IDSL and 804 IDSL Routers

Cisco IOS Firewall Feature Set is not new to Release 12.0(5)T; however, the Cisco IOS Firewall Feature Set combined with IPSec is new to this release. Enhancements to the Cisco IOS Firewall feature set are now available on the Cisco 802 IDSL and 804 IDSL routers. This feature set is available on the IP/Internet DSL/FW/IPSec56 and IP/Internet DSL/IPX/FW/ IPSec56 images only. This feature set provides the following additional capabilities:

- Context Based Access Control (CBAC)
- Java Blocking
- Denial of Service
- Real-time Alerts and Audit Trails

The *Cisco IOS Firewall Feature Set* feature module provides several sample firewall configurations, including the following examples for small-office environments:

- IP network to Internet
- Remote office network to corporate office network

If you want to configure a firewall in an IP-network-to-Internet network, you can use the Cisco 800 Fast Step application (recommended for inexperienced network administrators) or the Cisco IOS software command-line interface (CLI) (recommended for more experienced network administrators). You can also configure a firewall by using Cisco ConfigMaker software version 2.3.

With the Cisco 800 Fast Step application, you can configure CBAC only. For information on how to use the Cisco 800 Fast Step application, refer to the application online help.

If you want to configure a firewall in a remote-office-to-corporate-office network, you must use the Cisco IOS CLI. For information on how to configure a firewall using the CLI, refer to the following online documents:

- *Cisco IOS Firewall Feature Set* feature module document
- *Security Configuration Guide*
- *Security Command Reference*

IPSec Network Security

The IPSec network security feature is now available on the Cisco 802 IDSL and 804 IDSL routers (IP/Internet DSL/FW/IPSec56 and IP/Internet DSL/IPX/FW/ IPSec56 images only). This feature supports the 56-bit Data Encryption Standard (DES); it does not support the triple DES. Enabling this feature can impact your router performance.

IPSec is a framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers, such as two routers. IPSec provides these security services on IP datagrams. For information on configuring this feature, refer to the *Cisco IOS Release 12.0 Security Configuration Guide*.

Layer Two Tunneling Protocol (L2TP)

Layer Two Tunneling Protocol (L2TP) is an emerging Internet Engineering Task Force (IETF) standard that combines the best features of two existing tunneling protocols: Cisco's Layer Two Forwarding (L2F) and Microsoft's Point-to-Point Tunneling Protocol (PPTP). L2TP is an extension to the Point-to-Point Protocol (PPP), which is an important component for Access Virtual Private Networks (VPNs). Access VPNs allow mobile users to connect to their corporate intranets or extranets, thus improving flexibility and reducing costs.

Traditional dial-up networking services only supported registered IP address, which limited the types of applications that could be implemented over Virtual Private Networks (VPNs). L2TP supports multiple protocols and unregistered and privately administered IP addresses over the Internet. This allows the existing access infrastructure, such as the Internet, modems, access servers, and ISDN terminal adaptors (TAs), to be used. L2TP can be initiated wherever PPTP or L2F is currently deployed and can be operated as a client initiated tunnel, such as PPTP, or a network access server (NAS) initiated tunnel, such as L2F.

New Software Features in Release 12.0(4)T

The following new software enhancements are supported by the Cisco 802 IDSL and 804 IDSL routers in Release 12.0(4)T1 and later releases.

Cisco IOS Firewall Feature Set for the Cisco 802 IDSL and 804 IDSL Routers

The Cisco IOS Firewall feature set is now available on the Cisco 802 IDSL and 804 IDSL routers. This feature set is available on the IP/Firewall image only; the product code for this image is S8CH-12.0(4)T. This feature set provides the following capabilities:

- Context-based Access Control (CBAC)
- Java blocking
- Denial-of-service detection and prevention
- Real-time alerts and audit trails

The *Cisco IOS Firewall Feature Set* feature module provides several sample firewall configurations, including the following examples for small-office environments:

- IP network to Internet
- Remote office network to corporate office network

If you want to configure a firewall in an IP-network-to-Internet network, you can use the Cisco 800 Fast Step application (recommended for inexperienced network administrators) or the Cisco IOS software command-line interface (CLI) (recommended for more experienced network administrators). You can also configure a firewall by using Cisco ConfigMaker software version 2.3.

With the Cisco 800 Fast Step application, you can configure CBAC only. If you want to configure a firewall in a remote-office-to-corporate-office network, you must use the Cisco IOS CLI.

For information on how to use the Cisco 800 Fast Step application, refer to the application online help. For information on how to configure a firewall using the CLI, refer to the *Cisco IOS Firewall Feature Set* feature module. (See the “Feature Modules” section on page 19.)

New Features in Release 12.0(3)T

Cisco IOS Release 12.0(3)T was the first 12.0 T release to support Cisco 802 IDSL and 804 IDSL routers. The following new software enhancements, which were introduced in Release 12.0(1)T, are supported by the Cisco 802 IDSL and 804 IDSL routers beginning in this release.

Easy IP Phase 2-DHCP Server

With the introduction of Easy IP Phase 2, Cisco IOS software also supports Intelligent DHCP Relay functionality. A DHCP Relay Agent is any host that forwards DHCP packets between clients and servers. A DHCP Relay Agent enables the client and server to reside on separate subnets. If the Cisco IOS DHCP server cannot satisfy a DHCP request from its own database, it can forward the DHCP request to one or more secondary DHCP servers defined by the network administrator using standard Cisco IOS ip helper-address functionality.

Time-Based Access Lists

It is now possible to implement access lists based on the time of day. To do so, you create a time range that defines specific times of the day and week. The time range is identified by a name, and then referenced by a function, so that those time restrictions are imposed on the function itself.

Currently, IP and IPX extended access lists are the only functions that can use time ranges. The time range allows the network administrator to define when the permit or deny statements in the access list are in effect. Prior to this feature, access list statements were always in effect once they were applied. Both named or numbered access lists can reference a time range.

RIP Enhancements

Triggered extensions to IP RIP increase efficiency of RIP on point-to-point, serial interfaces. Routers are used on connection-oriented networks to allow potential connectivity to many remote destinations. Circuits on the WAN are established on demand and are relinquished when the traffic subsides. Depending on the application, the connection between any two sites for user data could be short and relatively infrequent.

There were two problems using RIP to connect to a WAN:

- Periodic broadcasting by RIP generally prevented WAN circuits form being closed.
- Even on fixed, point-to-point links, the overhead of periodic RIP transmissions could seriously interrupt normal data transfer because of the quantity of information that hits the line every 30 seconds.

To overcome these limitations, triggered extensions to RIP cause RIP to send information on the WAN only when there has been an update to the routing database. Periodic update packets are suppressed over the interface on which this feature is enabled.

ISDN MIB RFC2127

The new Integrated Services Digital Network (ISDN) Management Information Base (MIB) RFC2127 has been designed to provide useful information in accordance with the IETF's new standard for the management of ISDN interfaces. It controls all aspects of ISDN interfaces. RFC2127 provides information on the physical Basic Rate Interfaces (BRIs), control and statistical information for B (bearer) and D (signaling) channels, terminal endpoints, and directory numbers.

Important Notes

The following sections contain important notes about Cisco IOS Release 12.0 that can apply to the Cisco 802 IDSL and 804 IDSL routers.

Cisco ConfigMaker Installation and Configuration Tool

Cisco ConfigMaker is designed to substantially reduce the time required to configure multiple network devices. Through an easy-to-use graphical user interface, ConfigMaker allows you to draw your network, configure multiple network devices and set Cisco IOS® parameters. Plus, ConfigMaker will verify the accuracy of each device configuration to ensure interoperability. ConfigMaker ships free with Cisco routers and is backed by Cisco's highly acclaimed customer service and support organization.

For more information or to download a free copy of ConfigMaker, go to http://www.cisco.com/warp/public/cc/cisco/mkt/enm/config/.

Cisco IOS Release 12.0(4)XM

The images introduced in Release 12.0(4)XM apply to the Cisco 805 router *only.* They are not supported by the Cisco 801, 802, 803 or 804. For more information about this special release, see the *Release Notes for the Cisco 805 Router for Cisco IOS Release 12.0(4)XM* on CCO.

Hanging During Boot

If an illegal console configuration is issued to the router, the console fails the POST tests during bootup and causes the router to halt. There is no way to recover a system in this state except for pulling the soldered Boot Flash and re-burning the Boot ROM.

This problem has been resolved in TinyROM version 1.0(3), a downloadable ROM upgrade available from CCO. Please contact Cisco to upgrade to this version or later, and prevent this problem from occurring.

NVRAM Data Storage Limitation in Release 12.0(4)T and Earlier

The Cisco 800 router nonvolatile RAM (NVRAM) has a configuration data storage limitation in Cisco IOS Release 12.0(4)T and earlier releases. This problem was resolved in Release 12.0(5)T. Because of this limitation, you might not be able to save the digital certificate into the NVRAM if a large amount of other configuration data already exists. Cisco recommends that you not power off your router if you are not able to save the digital certificate. If you power off your router without successfully saving the digital certificate, you will need to generate the keys and request a new digital certificate from the Certificate Authority (CA) server after powering on the router again.

Cisco IOS Syslog Failure

Certain versions of Cisco IOS software may fail or hang when they receive invalid User Datagram Protocol (UDP) packets sent to their syslog ports (port 514). At least one commonly used Internet scanning tool generates packets that cause such problems. This fact has been published on public Internet mailing lists, which are widely read both by security professionals and by security crackers. This information should be considered in the public domain.

Attackers can cause Cisco IOS devices to repeatedly fail and reload, resulting in a completely disabled Cisco IOS device that needs to be reconfigured by its administrator. Some Cisco IOS devices have been observed to hang instead of failing when attacked. These devices do not recover until they are manually restarted by reset or power cycling. An administrator must personally visit an attacked, hung device to restart it, even if the attacker is no longer actively sending any traffic. Some devices have failed without providing stack traces; some devices may indicate that they were “restarted by power-on,” even when that is not the case.

Assume that any potential attacker is likely to know that existence of this problem and the ways to exploit it. An attacker can use tools available to the public on the Internet and does not need to write any software to exploit the vulnerability. Minimal skill is required and no special equipment is required.

Despite Cisco specifically inviting such reports, Cisco has received no actual reports of malicious exploitation of this problem.

This vulnerability notice was posted on Cisco’s World Wide Web site:

http://www.cisco.com/warp/public/770/iossyslog-pub.shtml

This information was also sent to the following e-mail and USENET news recipients:

- cust-security-announce@cisco.com
- bugtraq@netspace.org
- first-teams@first.org (includes CERT/CC)
- first-info@first.org
- cisco@spot.colorado.edu
- comp.dcom.sys.cisco
- nanog@merit.edu

Affected Devices and Software Versions

Vulnerable devices and software versions are specified in Table 5, *Affected and Repaired Software Versions.* Affected versions include Releases 11.3 AA, 11.3 DB, and all 12.0 versions (including 12.0 mainline, 12.0 S, 12.0 T, and any other regular released version whose number starts with 12.0), up to the repaired releases listed in Table 5. Cisco is correcting the problem in certain special releases and will correct it in future maintenance and interim releases. See Table 5, *Affected and Repaired Software Versions* for details. Cisco intends to provide fixes for all affected IOS variants.

No particular configuration is needed to make a Cisco IOS device vulnerable. It is possible to filter out attack traffic by using access lists. See the “Workarounds” section on page 14 for techniques. However, except at Internet firewalls, the appropriate filters are not common in customer configurations. Carefully evaluate your configuration before assuming that any filtering you have protects you against this attack.

The most commonly used or asked-about products are listed below. If you are unsure whether your device is running Cisco IOS software, log in to the device and issue the **show version** command. Cisco IOS software will identify itself simply as "IOS" or "Internetwork Operating System Software". Other Cisco devices will not have the **show version** command, or they will identify themselves differently in their output. The most common Cisco devices that run Cisco IOS software include the following:

- Cisco routers in the AGS/MGS/CGS/AGS+, IGS, RSM, 800, uBR900, 1000, 2500, 2600, 3000, 3600, 3800, 4000, 4500, 4700, AS5200, AS5300, AS5800, 6400, 7000, 7200 (including the uBR7200), 7500, and 12000 series
- Most recent versions of the LS1010 ATM switch
- Some versions of the Catalyst 2900XL LAN switch
- Cisco DistributedDirector

Affected software versions, which are relatively new, are not necessarily available on every device listed above. If you are not running Cisco IOS software, you are not affected by this problem.

The following Cisco devices are *not* affected:

- 700 dialup routers (750, 760, and 770 series)
- Catalyst 1900, 2800, 2900, 3000, and 5000 LAN switches are not affected, except for some versions of the Catalyst 2900XL. However, optional router modules running Cisco IOS software in switch backplanes, such as the RSM module for the Catalyst 5000 and 5500, are affected.
- WAN switching products in the IGX and BPX lines
- MGX (formerly known as the AXIS shelf)
- Host-based software
- Cisco PIX Firewall
- Cisco LocalDirector
- Cisco Cache Engine

This vulnerability has been assigned Cisco bug ID CSCdk77426.

Solution

Cisco offers free software updates to correct this vulnerability for all affected customers—regardless of their contract status. However, because this vulnerability information has been disseminated by third parties, Cisco has released this notice before updates are available for all software versions. Table 5 gives Cisco's projected fix dates.

Make sure your hardware has adequate RAM to support the new software before installing it. The amount of RAM is seldom a problem when you upgrade within a major release (say, from 11.2[11]P to 11.2[17]P), but it is often a factor when you upgrade between major releases (say, from 11.2 P to 11.3 T).

Because fixes will be available for all affected releases, this vulnerability will rarely, if ever, require an upgrade to a new major release. Cisco recommends very careful planning for any upgrade between major releases. Make certain no known bugs will prevent the new software from working properly in your environment.

Further upgrade planning assistance is available on Cisco's World Wide Web site at:

http://www.cisco.com

If you have service contracts you can obtain new software through your regular update channels (generally through Cisco's World Wide Web site). You can upgrade to any software release, but you must remain within the boundaries of the feature sets you have purchased.

If you do not have service contracts, you can upgrade to obtain only the bug fixes; free upgrades are restricted to the minimum upgrade required to resolve the defects. In general, you will be restricted to upgrading within a single row of Table 5, except when no upgrade within the same row is available in a timely manner. Obtain updates by contacting one of the following Cisco Technical Assistance Centers (TACs):

- +1 800 553 2447 (toll-free from within North America)
- +1 408 526 7209 (toll call from anywhere in the world)
- tac@cisco.com

Give the URL of this notice (http://www.cisco.com/warp/public/770/iossyslog-pub.shtml) as evidence for a free update. Non-contract customers must request free updates through the TAC. Please do not contact either "psirt@cisco.com" or "security-alert@cisco.com" for software updates.

Workarounds

You can work around this vulnerability by preventing any affected Cisco IOS device from receiving or processing UDP datagrams addressed to its port 514. This can be done either by using packet filtering on surrounding devices, or by using input access list filtering on the affected IOS device itself.

If you use an input access list, apply that list to all interfaces to which attackers may be able to send datagrams. Interfaces include not only physical LAN and WAN interfaces but also virtual subinterfaces of those physical interfaces, as well as virtual interfaces and interface templates corresponding to GRE, L2TP, L2F, and other tunneling protocols.

The input access list must block traffic destined for UDP port 514 at any of the Cisco IOS device's own IP addresses, as well as at any broadcast or multicast addresses on which the Cisco IOS device may be listening. Be sure to block both old-style "all-zeros" broadcasts and new-style "all-ones" broadcasts. It is not necessary to block traffic being forwarded to other hosts—only traffic actually addressed to the Cisco IOS device is of interest.

No single input access list works in all configurations. Know the effect of your access list in your specific configuration before activating it.

The following example shows a possible access list for a three-interface router, along with the configuration commands needed to apply the list. The example assumes input filtering is not needed, other than as a workaround for this problem:

```
! Deny all multicasts, and all unspecified-net broadcasts, to port 514
access-list 101 deny udp any 224.0.0.0 31.255.255.255 eq 514
! Deny old-style unspecified-net broadcasts
access-list 101 deny udp any host 0.0.0.0 eq 514
! Deny network-specific broadcasts. This example assumes that all of
! the local interfaces are on the class B network 172.16.0.0, subnetted
! everywhere with mask 255.255.255.0. This will differ from network
! to network. Note that we block both new-style and old-style broadcasts.
access-list 101 deny udp any 172.16.0.255 0.0.255.0 eq 514
access-list 101 deny udp any 172.16.0.0   0.0.255.0 eq 514
! Deny packets sent to the addresses of our own network interfaces.
access-list 101 deny udp any host 172.16.1.1 eq 514
access-list 101 deny udp any host 172.16.2.1 eq 514
access-list 101 deny udp any host 172.16.3.3 eq 514
! Permit all other traffic (default would be to deny)
access-list 101 permit ip any any

! Apply the access list to the input side of each interface
interface ethernet 0
ip address 172.16.1.1 255.255.255.0
ip access-group 101 in

interface ethernet 2
ip address 172.16.2.1 255.255.255.0
ip access-group 101 in

interface ethernet 3
ip address 172.16.3.3 255.255.255.0
ip access-group 101 in
```

Listing all possible addresses—especially all possible broadcast addresses—to which attack packets may be sent is complicated. If you do not need to forward any legitimate syslog traffic received on an interface, you can block all syslog traffic arriving on that interface. Remember that blocking will affect traffic routed through the Cisco IOS device as well as traffic destined to the device; if the IOS device is expected to forward syslog packets, you will have to do the detailed filtering. Because input access lists impact system performance, install them with caution—especially on systems running very near their capacity.

Software Versions and Fixes

Many Cisco software images have been or will be specially reissued to correct this vulnerability. For example, regular released Cisco IOS version 12.0(2) is vulnerable, as are interim versions 12.0(2.1) through 12.0(2.3). The first fixed interim version of Release12.0 mainline software is Release12.0(2.4). However, a special release, 12.0(2a), contains only the fix for this vulnerability and does not include any other bug fixes from later 12.0 interim releases.

If you are running Release 12.0(2) and want to fix this problem without risking possible instability presented by installing the 12.0(2.4) interim release, you can upgrade to Release 12.0(2a). Release 12.0(2a) is a “code branch” from the Release 12.0(2) base, which will merge back into the Release 12.0 mainline at Release 12.0(2.4).

Special releases, like 12.0(2a), are one-time, spot fixes, and they will not be maintained. Thus, the upgrade path from Release 12.0(2a) is to Release 12.0(3).

Table 5 specifies information about affected and repaired software versions.

Note All dates within this table are subject to change.

Table 5 Affected and Repaired Software Versions

Cisco IOS Major Release	Description	Special Fix[1]	First Fixed Interim Release[2]	Fixed Maintenance Release[3]
Unaffected Releases				
11.2 and earlier releases—all variants	Unaffected early releases (no syslog server)	Unaffected	Unaffected	Unaffected
11.3, 11.3 T, 11.3 DA, 11.3 MA, 11.3 NA, 11.3 WA, 11.3(2)XA	11.3 releases without syslog servers	Unaffected	Unaffected	Unaffected
Releases Based on 11.3				
11.3 AA	11.3 early deployment for AS58xx	11.3(7)AA2, 8-JAN-1999[4]	11.3(7.2)AA	11.3(8)AA, 15-FEB-1999
11.3 DB	11.3 for Cisco NRP routing blade in Cisco 6400 xDSL DSLAM			11.3(7)DB2, 18-JAN-1999
Releases Based on 12.0				
12.0	12.0 Mainline	12.0(2a), 8-JAN-1999	12.0(2.4)	12.0(3), 1-FEB-1999
12.0 T	12.0 new technology early deployment	12.0(2a)T1, 11-JAN-1999	12.0(2.4)T	12.0(3)T, 15-FEB-1999
12.0 S	ISP support; 7200, RSP, GSR		12.0(2.3)S, 27-DEC-1998	12.0(2)S[5], 18-JAN-1999
12.0 DB	12.0 for Cisco 6400 universal access concentrator node switch processor (lab use)			12.0(2)DB, 18-JAN-1999
12.0(1)W	12.0 for Catalyst 8500 and LS1010	12.0(1)W5(5a) and 12.0(1a)W5(5b) (LS1010 platform only)	12.0(1)W5(5.15)	12.0(1)W5(6) (platform support for Catalyst 8540M will be in 12.0(1)W5(7))
12.0(0.6)W5	One-time early deployment for CH-OC-12 module in Catalyst 8500 series switches	Unaffected; one-time release	Unaffected	Unaffected; To upgrade use 12.0(1)W5 releases.
12.0(1)XA3	Short-life release; merged to 12/0T at 12.0(2)T	Obsolete	Merged	Upgrade to 12.0(2a)T1 or to 12.0(3)T.
12.0(1)XB	Short-life release for Cisco 800 series; merged to 12.0 T and 12.0 (3)T	12.0(1)XB1	Merged	Upgrade to 12.0(3)T.

Table 5 Affected and Repaired Software Versions (continued)

Cisco IOS Major Release	Description	Special Fix[1]	First Fixed Interim Release[2]	Fixed Maintenance Release[3]
12.0(2)XC	Short-life release for new features in Cisco 2600, Cisco 3600, uBR7200, uBR900 series; merged to 12.0 T at 12.0(3)T	12.0(2)XC1, 7-JAN-1999	Merged	Upgrade to 12.0(3)T
12.0(2)XD	Short-life release for ISDN voice features; merged to 12.0 T at 12.0(3)T	12.0(2)XD1, 18-JAN-1999	Merged	Upgrade to 12.0(3)T
12.0(1)XE	Short-life release	12.0(2)XE, 18-JAN-1999	Merged	Upgrade to 12.0(3)T

1. A special fix is a one-time release that provides the most stable immediate upgrade path.
2. Interim releases are tested less rigorously than regular maintenance releases; interim releases can contain serious bugs.
3. Fixed maintenance releases are on a long-term upgrade path. Other long-term upgrade paths also exist.
4. All dates in this table are estimates and are subject to change.
5. This entry is not a misprint. The 12.0(2.3)S interim release is available before the 12.0(2)S regular release.

Caveats

Caveats describe unexpected behavior in Cisco IOS software releases. Severity 1 caveats are the most serious caveats; severity 2 caveats are less serious.

This section only contains open and resolved caveats for the current Cisco IOS maintenance release. All caveats in Release 12.0 T are also in Release 12.0.

For information on caveats in Cisco IOS Release 12.0, see *Caveats for Cisco IOS Release 12.0*. For information on caveats in Cisco IOS Release 12.0 T, see *Caveats for Cisco IOS Release 12.0 T*, which lists severity 1 and 2 caveats and is located on CCO and the Documentation CD-ROM.

Note If you have an account with CCO, you can use Bug Navigator II to find caveats of any severity for any release. You can reach Bug Navigator II on CCO at **Software Center**: **Cisco IOS Software**: **BUG TOOLKIT**: **Cisco Bug Navigator II**, or at http://www.cisco.com/support/bugtools/bugtool.shtml.

Related Documentation

The following sections describe the documentation available for the Cisco 802 IDSL and 804 IDSL routers. These documents consist of hardware and software installation guides, Cisco IOS configuration and command references, system error messages, feature modules, and other documents. Documentation is available as printed manuals or electronic documents, except for feature modules, which are available online on CCO and the Documentation CD-ROM.

Use these release notes with the documents listed in the following sections:

- Release-Specific Documents, page 18
- Platform-Specific Documents, page 19
- Feature Modules, page 19
- Cisco IOS Software Documentation Set, page 19

Release-Specific Documents

The following documents are specific to Release 12.0. They are located on CCO and the Documentation CD-ROM:

- *Release Notes for Cisco IOS Release 12.0*
  - To reach the *Cross-Platform Release Notes for Cisco IOS Release 12.0* from CCO, click on this path (under the heading **Service & Support**):

    Technical Documents: **Documentation Home Page**: **Cisco IOS Software Configuration**: **Cisco IOS Release 12.0**: **Release Notes**: **Cross-Platform Release Notes**
  - To reach the *Cross-Platform Release Notes for Cisco IOS Release 12.0* on the Documentation CD-ROM, click on this path:

    Cisco Product Documentation: Cisco IOS Software Configuration: **Cisco IOS Release 12.0**: **Release Notes**: **Cross-Platform Release Notes**
- Product bulletins, field notices, and other release-specific documents

  To reach these documents from CCO, click on this path (under the heading **Service & Support**):

  Technical Documents: **Product Bulletins**
- *Caveats for Cisco IOS Release 12.0 T*

  As a supplement to the caveats listed in the "Caveats" section on page 17 section in these release notes, see the *Caveats for Cisco IOS Release 12.0* and *Caveats for Cisco IOS Release 12.0 T* documents, which contains caveats applicable to all platforms for all maintenance releases of Release 12.0.
  - To reach the caveats document from CCO, click on this path (under the heading **Service & Support**):

    Technical Documents: **Documentation Home Page**: **Cisco IOS Software Configuration**: **Cisco IOS Release 12.0**: **Caveats**
  - To reach the caveats document on the Documentation CD-ROM, click on this path:

    Cisco Product Documentation: **Cisco IOS Software Configuration**: **Cisco IOS Release 12.0**: **Caveats**

Note If you have an account with CCO, you can use Bug Navigator II to find caveats of any severity for any release. You can reach Bug Navigator II on CCO at **Software Center**: **Cisco IOS Software**: **BUG TOOLKIT**: **Cisco Bug Navigator II**, or at http://www.cisco.com/support/bugtools/bugtool.shtml.

Platform-Specific Documents

These documents are available for the Cisco 802 IDSL and 804 IDSL routers on CCO and the Documentation CD-ROM.

- *Cisco 800 Series Routers Hardware Installation Guide*
- *Quick Start Guide — Setting up Cisco 800 Series Routers*
- *Regulatory Compliance and Safety Info For Cisco 800 Series*
- *Cisco 800 Series Routers Software Configuration Guide*
- *Cisco 800 Fast Step Quick Start Guide*
- *Upgrading Memory in the Cisco 800 Series Routers*
- *Release Notes for Cisco 800 Series Routers*

To reach Cisco 800 series documentation from CCO, click on this path (under the heading **Service & Support**):

Technical Documents: **Documentation Home Page**: **Access Servers and Access Routers**: **Fixed Access Routers**: **Cisco 800 series**

To reach Cisco 800 series documentation on the Documentation CD-ROM, click on this path:

Cisco Product Documentation: **Access Servers and Access Routers**: **Fixed Access Routers**: **Cisco 800 series**

Feature Modules

Feature modules describe new features supported by Release 12.0 T and are updates to the Cisco IOS documentation set. A feature module consists of a brief overview of the feature, benefits, configuration tasks, and a command reference. As updates, the feature modules are available online only. Feature module information is incorporated in the next printing of the Cisco IOS documentation set.

To reach the feature modules from CCO, click on this path (under the heading **Service & Support**):

Technical Documents: **Documentation Home Page**: **Cisco IOS Software Configuration**: **Cisco IOS Release 12.0**: **New Feature Documentation**

To reach the feature modules on the Documentation CD-ROM, click on this path:

Cisco Product Documentation: **Cisco IOS Software Configuration**: **Cisco IOS Release 12.0**: **New Feature Documentation**

Cisco IOS Software Documentation Set

The Cisco IOS software documentation set consists of the Cisco IOS configuration guides, Cisco IOS command references, and several other supporting documents that are shipped with your order in electronic form on the Documentation CD-ROM—unless you specifically ordered the printed versions.

Documentation Modules

Each module in the Cisco IOS documentation set consists of two books: a configuration guide and a corresponding command reference. Chapters in a configuration guide describe protocols, configuration tasks, Cisco IOS software functionality, and contain comprehensive configuration examples. Chapters

in a command reference provide complete command syntax information. Use each configuration guide with its corresponding command reference. On CCO and the Documentation CD-ROM, two master hot-linked documents provide information for the Cisco IOS software documentation set.

On CCO (under the heading **Service & Support**):

Technical Documents: **Documentation Home Page**: **Cisco IOS Software Configuration**: **Cisco IOS Release 12.0**: **Configuration Guides and Command References**

On the Documentation CD-ROM:

Cisco Product Documentation: **Cisco IOS Software Configuration**: **Cisco IOS Release 12.0**: **Configuration Guides and Command References**

Release 12.0 Documentation Set

Table 6 describes the contents of the Cisco IOS Release 12.0 software documentation set, which is available in electronic form and in printed form upon request.

Note You can find the most current Cisco IOS documentation on CCO and the Documentation CD-ROM. These electronic documents may contain updates and modifications made after the hard-copy documents were printed.

On CCO at (under the heading **Service & Support**):

Technical Documents: **Documentation Home Page**: **Cisco IOS Software Configuration**: **Cisco IOS Release 12.0**

On the Documentation CD-ROM at:

Cisco Product Documentation: **Cisco IOS Software Configuration**: **Cisco IOS Release 12.0**

Table 6 Cisco IOS Software Release 12.0 Documentation Set

Books	Chapter Topics
• *Configuration Fundamentals Configuration Guide* • *Configuration Fundamentals Command Reference*	Configuration Fundamentals Overview Cisco IOS User Interfaces File Management System Management
• *Bridging and IBM Networking Configuration Guide* • *Bridging and IBM Networking Command Reference*	Transparent Bridging Source-Route Bridging Token Ring Inter-Switch Link Remote Source-Route Bridging DLSw+ STUN and BSTUN LLC2 and SDLC IBM Network Media Translation DSPU and SNA Service Point SNA Frame Relay Access Support APPN Cisco Database Connection NCIA Client/Server Topologies Cisco Mainframe Channel Connection Airline Product Set

Table 6 Cisco IOS Software Release 12.0 Documentation Set (continued)

Books	Chapter Topics
• *Dial Solutions Configuration Guide* • *Dial Solutions Command Reference*	X.25 over ISDN Appletalk Remote Access Asynchronous Callback, DDR, PPP, SLIP Bandwidth Allocation Control Protocol ISDN Basic Rate Service ISDN Caller ID Callback PPP Callback for DDR Channelized E1 & T1 Dial Backup for Dialer Profiles Dial Backup Using Dialer Watch Dial Backup for Serial Lines Peer-to-Peer DDR with Dialer Profiles DialOut Dial-In Terminal Services Dial-on-Demand Routing (DDR) Dial Backup Dial-Out Modem Pooling Large-Scale Dial Solutions Cost-Control Solutions Virtual Private Dialup Networks Dial Business Solutions and Examples
• *Cisco IOS Interface Configuration Guide* • *Cisco IOS Interface Command Reference*	Interface Configuration Overview LAN Interfaces Logical Interfaces Serial Interfaces
• *Network Protocols Configuration Guide, Part 1* • *Network Protocols Command Reference, Part 1*	IP Overview IP Addressing and Services IP Routing Protocols
• *Network Protocols Configuration Guide, Part 2* • *Network Protocols Command Reference, Part 2*	AppleTalk Novell IPX
• *Network Protocols Configuration Guide, Part 3* • *Network Protocols Command Reference, Part 3*	Network Protocols Overview Apollo Domain Banyan VINES DECnet ISO CLNS XNS
• *Security Configuration Guide* • *Security Command Reference*	AAA Security Services Security Server Protocols Traffic Filtering and Firewalls IP Security and Encryption Passwords and Privileges Neighbor Router Authentication IP Security Options
• *Cisco IOS Switching Services Configuration Guide* • *Cisco IOS Switching Services Command Reference*	Switching Services Switching Paths for IP Networks Virtual LAN (VLAN) Switching and Routing

Table 6 Cisco IOS Software Release 12.0 Documentation Set (continued)

Books	Chapter Topics
• *Wide-Area Networking Configuration Guide* • *Wide-Area Networking Command Reference*	Wide-Area Network Overview ATM Frame Relay SMDS X.25 and LAPB
• *Voice, Video, and Home Applications Configuration Guide* • *Voice, Video, and Home Applications Command Reference*	Voice over IP Voice over Frame Relay Voice over ATM Voice over HDLC Frame Relay-ATM Internetworking Synchronized Clocks Video Support Universal Broadband Features
• *Quality of Service Solutions Configuration Guide* • *Quality of Service Solutions Command Reference*	Policy-Based Routing QoS Policy Propagation via BGP Committed Access Rate Weighted Fair Queueing Custom Queueing Priority Queueing Weighted Random Early Detection Scheduling Signaling RSVP Packet Drop Frame Relay Traffic Shaping Link Fragmentation RTP Header Compression
• *Cisco IOS Software Command Summary* • *Dial Solutions Quick Configuration Guide* • *System Error Messages* • *Debug Command Reference*	

Note *Cisco Management Information Base (MIB) User Quick Reference* is no longer published. For the latest list of MIBs supported by Cisco, see *Cisco Network Management Toolkit* on Cisco Connection Online. From CCO, click on the following path: **Service & Support**: **Software Center**: **Network Mgmt Products**: **Cisco Network Management Toolkit**: **Cisco MIB**.

Service and Support

For service and support for a product purchased from a reseller, contact the reseller, who offers a wide variety of Cisco service and support programs described in "Service and Support" of *Cisco Information Packet* that shipped with your product.

Note If you purchased your product from a reseller, you can access CCO as a guest. CCO is Cisco Systems' primary real-time support channel. Your reseller offers programs that include direct access to CCO services.

For service and support for a product purchased directly from Cisco, use CCO.

Software Configuration Tips on the Cisco Technical Assistance Center Home Page

If you have a CCO login account, you can access the following URL, which contains links and tips on configuring your Cisco products:

http://www.cisco.com/kobayashi/serv_tips.shtml

This URL is subject to change without notice. If it changes, point your Web browser to CCO and click on this path: **Products & Technologies**: **Products**: **Technical Tips.**

The following sections are provided from the Technical Tips page:

- Access Dial Cookbook—Contains common configurations or recipes for configuring various access routes and dial technologies.
- Field Notices—Notifies you of any critical issues regarding Cisco products and includes problem descriptions, safety or security issues, and hardware defects.
- Frequently Asked Questions—Describes the most frequently asked technical questions about Cisco hardware and software.
- Hardware—Provides technical tips related to specific hardware platforms.
- Hot Tips—Describes popular tips and hints gathered from the Cisco Technical Assistance Center (TAC). Most of these documents are available from the TAC Fax-on-demand service. To reach Fax-on-demand and receive documents at your fax machine from the United States, call 888-50-CISCO (888-502-4726). From other areas, call 650-596-4408.
- Internetworking Features—Lists tips on using Cisco IOS software features and services.
- Sample Configurations—Provides actual configuration examples that are complete with topology and annotations.
- Software Products—Contains Cisco IOS Software Bulletins, Cisco TCP/IP Suite 100, General Cisco IOS, Internet/Intranet Applications and Software, Network Management, Network Protection Software Tips, and WAN Switching Products and Software.
- Special Collections—Lists other helpful documents, including Case Studies, References & Request for Comments (RFCs), and Security Advisories.

Cisco Connection Online

Cisco Connection Online (CCO) is Cisco Systems' primary, real-time support channel. Maintenance customers and partners can self-register on CCO to obtain additional information and services.

Available 24 hours a day, 7 days a week, CCO provides a wealth of standard and value-added services to Cisco's customers and business partners. CCO services include product information, product documentation, software updates, release notes, technical tips, the Bug Navigator, configuration notes, brochures, descriptions of service offerings, and download access to public and authorized files.

CCO serves a wide variety of users through two interfaces that are updated and enhanced simultaneously: a character-based version and a multimedia version that resides on the World Wide Web (WWW). The character-based CCO supports Zmodem, Kermit, Xmodem, FTP, and Internet e-mail, and it is excellent for quick access to information over lower bandwidths. The WWW version of CCO provides richly formatted documents with photographs, figures, graphics, and video, as well as hyperlinks to related information.

You can reach CCO in the following ways:

- WWW: http://www.cisco.com
- WWW: http://www-europe.cisco.com
- WWW: http://www-china.cisco.com
- Telnet: cco.cisco.com
- Modem: From North America, 408 526-8070; from Europe, 33 1 64 46 40 82. Use the following terminal settings: VT100 emulation; databits: 8; parity: none; stop bits: 1; and connection rates up to 28.8 kbps.

For a copy of CCO's Frequently Asked Questions (FAQ), contact cco-help@cisco.com. For additional information, contact cco-team@cisco.com.

Note If you are a network administrator and need personal technical assistance with a Cisco product that is under warranty or covered by a maintenance contract, contact Cisco's Technical Assistance Center (TAC) at 800 553-2447, 408 526-7209, or tac@cisco.com. To obtain general information about Cisco Systems, Cisco products, or upgrades, contact 800 553-6387, 408 526-7208, or cs-rep@cisco.com.

Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which package that ships with your product. The Documentation CD-ROM, a member of the Cisco Connection Family, is updated monthly. Therefore, it might be more current than printed documentation. To order additional copies of the Documentation CD-ROM, contact your local sales representative or call customer service. The CD-ROM package is available as a single package or as an annual subscription. You can also access Cisco documentation on the World Wide Web at http://www.cisco.com, http://www-china.cisco.com, or http://www-europe.cisco.com.

If you are reading Cisco product documentation on the World Wide Web, you can submit comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco. We appreciate your comments.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section on page 17.

Access Registrar, AccessPath, Any to Any, AtmDirector, CCDA, CCDE, CCDP, CCIE, CCNA, CCNP, CCSI, CD-PAC, the Cisco logo, Cisco Certified Internetwork Expert logo, *CiscoLink*, the Cisco Management Connection logo, the Cisco Net*Works* logo, the Cisco Powered Network logo, Cisco Systems Capital, the Cisco Systems Capital logo, Cisco Systems Networking Academy, the Cisco Systems Networking Academy logo, the Cisco Technologies logo, ConnectWay, Fast Step, FireRunner, GigaStack, IGX, Internet Quotient, Kernel Proxy, MGX, MultiPath Data, MultiPath Voice, Natural Network Viewer, NetSonar, Network Registrar, *Packet*, PIX, Point and Click Internetworking, Policy Builder, Precept, Secure Script, ServiceWay, SlideCast, SMARTnet, *The Cell*, TrafficDirector, TransPath, ViewRunner, Virtual Service Node, VisionWay, VlanDirector, WebViewer, Workgroup Director, and Workgroup Stack are trademarks; Changing the Way We Work, Live, Play, and Learn, Empowering the Internet Generation, The Internet Economy, and The New Internet Economy are service marks; and ASIST, BPX, Catalyst, Cisco, Cisco IOS, the Cisco IOS logo, Cisco Systems, the Cisco Systems logo, the Cisco Systems Cisco Press logo, Enterprise/Solver, EtherChannel, EtherSwitch, FastHub, FastLink, FastPAD, FastSwitch, GeoTel, IOS, IP/TV, IPX, LightStream, LightSwitch, MICA, NetRanger, Post-Routing, Pre-Routing, Registrar, StrataView Plus, Stratm, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. or its affiliates in the U.S. and certain other countries. All other trademarks mentioned in this document are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any of its resellers. (9910R)

Copyright © 1999, Cisco Systems, Inc.
All rights reserved.